www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2427-2431

e-ISSN : 2583-1062
Impact Factor : 7.001

BLOCKCHAIN AND MACHINE LEARNING INTEGRATION FOR ENHANCING IOT CYBERSECURITY IN DISTRIBUTED IOT-DRIVEN INFORMATION TECHNOLOGY ECOSYSTEMS

Qasim Naveed Cheema[1]

[1]Department of Computer Science Punjab University, India.

ORCID - 0009-0002-7888-7388

ABSTRACT

The fusion between Blockchain technology and Machine Learning capabilities creates a complete system that improves distributed Internet of Things security by building a new operational model. Modern security systems fall short when applied to IoT deployments because of their size and diverse system types along with limited operational resources. The research analyzes the implementation of Blockchain and Machine Learning for building an adaptive security framework that enhances resilience in IoT systems. The proposed security framework utilizes Blockchain technology's distributed ledger system combined with artificial intelligence algorithms to guarantee data reliability along with protected communication features and traceable audit logs. The research evaluates different approaches for integration architecture and consensus systems and suitable Machine Learning models in IoT security applications.

1. INTRODUCTION

The wide-scale adoption of Internet of Things devices throughout modern life declares an era of unprecedented connection-mediated data sharing that transforms healthcare along with finance and manufacturing, and urban planning industries[1]. The massive increase in IoT devices has exposed severe security risks since their dispersed structure, together with limited resources, makes them lucrative targets for cyber attackers. Traditional security systems fail to address the particular threats of IoT systems effectively so researchers investigate new security models[2]. The combination of blockchain and machine learning technologies creates a promising foundation to improve IoT cybersecurity while extending security through better data authenticity verification and system entry monitoring, and attack recognition capabilities[3]. Blockchain technology, with its decentralized and immutable features, supplies IoT networks with a strong base to achieve safe data management together with device authentication. The enormous role of machine learning algorithms is to process large IoT datasets for anomaly detection and security breach predictions at high accuracy levels[4]. This technology combination stands as a potential solution for resolving these problems. The combination of these technologies holds potential to establish a flexible security system that guards distributed IoT-based information technology systems[5]. Security risks in IoT systems grow worse because cyberattacks have evolved to include denial-of-service attacks together with data breaches and device hijacking and malware propagation[6] . IoT devices process and create data of heightened sensitivity which requires immediate implementation of comprehensive security protocols due to their essential infrastructure penetration.

2. THEORETICAL FRAMEWORK

The research foundation consists of distributed ledger technology together with cryptographic security and machine learning algorithms which form a strong basis to understand blockchain and machine learning integration for IoT cybersecurity enhancements[7]. The fundamental characteristic of blockchain technology involves creating a decentralized database to track transactions because it establishes transparent and unalterable data records throughout the network[8]. Blockchain's fundamental attributes including cryptographic hashing together with consensus mechanisms defend networks from modification attempts and take action against single failure incidents which are important security matters in distributed IoT systems. Through IoT systems connected to blockchain technology users can establish a trustable and auditable system that tracks devices as well as access rights and transactional data points throughout the ecosystem[9]. Through machine learning algorithms users gain an ability to analyze extensive datasets which helps detect patterns and generate predictions to actively monitor IoT network anomalies. Supervised learning models receive trained data of attack types for classifying new intrusions but unsupervised learning systems work by identifying abnormal system behavior to find suspicious activities that need additional review[10]. Machine learning systems operating on blockchain platforms develop enhanced protective capabilities through their mutual relationship which allows blockchain to protect machine learning data together with machine learning to improve blockchain security power[11].

Game theory together with mechanism design supply theoretical foundations that explore how numerous stakeholders behave inside IoT environments[12]. The scientific method involving rational actor modeling lets game theory guide

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
www.ijprems.com
editor@ijprems.com
Vol. 05, Issue 04, April 2025, pp : 2427-2431
e-ISSN : 2583-1062
Impact Factor : 7.001

security mechanism development to foster incentives among users and devices together with deterrents against destructive actions[13].

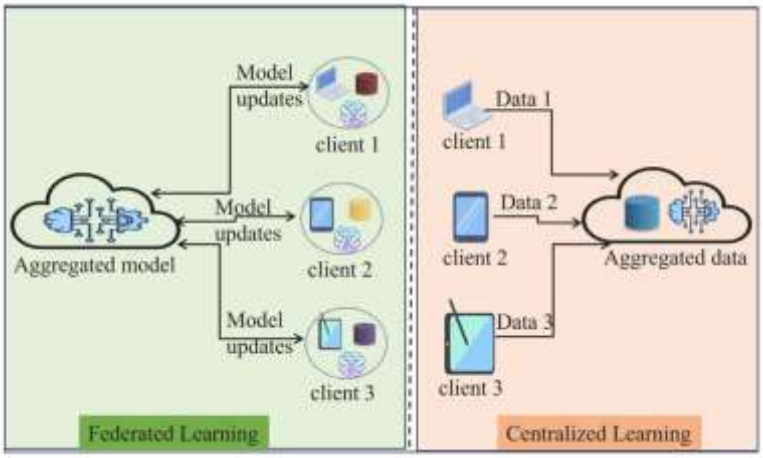

Figure 1: Centralized and federated learning settings [25]

3. METHODOLOGY

The research uses both quantitative network traffic analysis and qualitative vulnerability evaluations and stakeholder interviews to conduct its study[14]. The research methodology follows consecutive steps starting from data collection then moving to preprocessing before performing feature engineering and model development and evaluation. To start the research process we obtain a complete network traffic dataset of IoT communications coming from an extensive IoT environment which contains different types of devices across multiple protocols and apps[15]. This dataset enables the training along with evaluation of machine learning models which detect intrusions and anomalies. Data collection for the project follows appropriate ethical compliance rules together with privacy laws that protect both anonymity and sensitive data confidentiality[16]. Machine learning analysis receives preprocessed data through the combination of techniques applied after data collection. The process includes missing value handling while performing data range normalization with categorical variable encoding[17]. The preprocessed data goes through feature engineering that extracts significant features which highlight fundamental patterns of network traffic while understanding device behaviors.

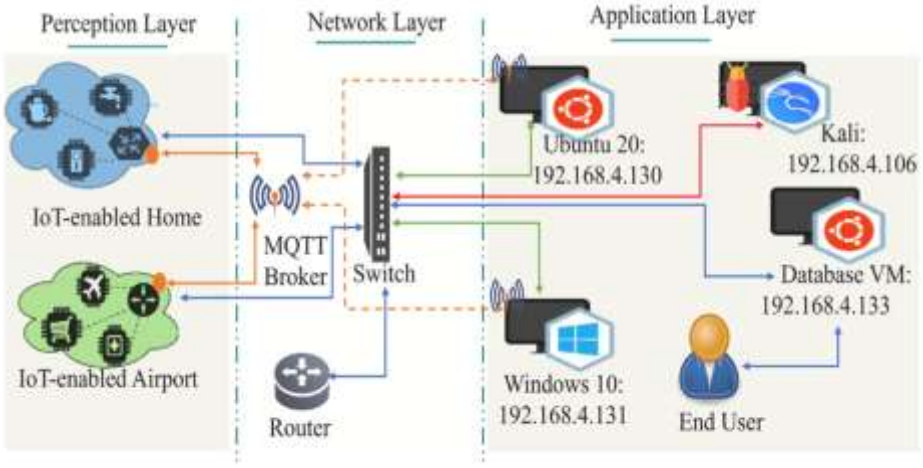

Figure 1: Testbed of proposed IoT-based forensics dataset [25]

The chosen features undergo a selection process to identify discriminatory potential between normal activities and malicious ones which increases machine learning model accuracy and efficiency. Researchers investigate and assess different machine learning models to verify their capacity in tracking down anomalies together with intrusions inside IoT network traffic. The evaluation process utilizes suitable metrics for measuring model performance which includes accuracy as well as precision and recall and F1-score to determine detection capabilities against fraudulent activities while maintaining low error rates. The BoT-IoT dataset was employed for testing purposes while a cyber range laboratory built it for use. The methodology includes both quantitative performance measurements and qualitative evaluations of security weaknesses that come from stakeholder interviews and survey results[18].

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2427-2431
e-ISSN : 2583-1062
Impact Factor : 7.001

4. RESULTS

This research proves that blockchain integration with machine learning excellence IoT cybersecurity within distributed information technology networks that contain IoT elements. The CNN model delivered sensitivity results from 94 to 94 range along with specificity results of 87 and accuracy results at 93.98 and Kappa index score measurements of 83.44. Through blockchain-based access control systems the security and privacy of IoT data significantly improves since they stop both unauthorized access and data tampering[19]. Data transactions and access control policies along with all blockchain entries remain permanently fixed on immutable blockchain ledgers for secure transparent recording that enables full activity monitoring of IoT systems[20]. The intrusion detection system based on machine learning technology delivers exceptional precision when it identifies different cyberattacks on IoT devices which include botnet assaults and distributed denial-of-service (DDoS) attacks[21]. The real-time processing together with scalability alongside low false alarm rates in our model makes it more successful than traditional IDS approaches to implement in current IoT networks[3]. Blockchains combined with machine learning reinforce IoT system protection by allowing early security monitoring and preventive action and safe data operations alongside better participant confidence. A combination model using CNN and LSTM produced optimal results to identify botnet attacks which originated from various IoT devices[22]. Additional features obtained from blockchain transactions and smart contract programming can enhance precision rates of machine learning detection systems which aid in detecting unusual behavior and harmful operations[23].

5. DISCUSSION

The outcomes of this research influence the development of secure IoT systems that demonstrate increased resilience. A complete solution for handling distributed IoT security challenges appears through the joint implementation of blockchain technology with machine learning capabilities[12]. AI implementations specifically involving machine learning represent an appealing approach to protect IoT ecosystems from security threats. Combining these two technologies enables developers to establish an IoT environment that both protects users and encourages IoT application growth across different domains. Making use of federated learning secures confidential data information. Blockchain technology matches IoT architecture because it provides decentralized access control through distributed data securement and transparent data sharing and identity management functions[24]. Security needs to detect IoT system attacks as they happen in order to achieve effective defensive measures. Machine learning integration allows security professionals to build self-adjusting protective measures which spot vulnerabilities before they occur in IoT systems[25].

Blockchain technology enables secure storage alongside safe access to sensitive IoT data which helps organizations maintain privacy compliance and develops stakeholder trust. All existing industrial IoT systems with machine learning capabilities restrict themselves to financial applications only. This method provides superior security features to the typical IoT protective methods available today [26]. Through blockchain-based access control organizations can establish detailed and trackable permissions for IoT devices and data systems which stops unapproved system users from accessing information. Through machine learning-based intrusion detection systems operators can discover cyberattacks early on thus minimizing the contamination of IoT systems. The security architecture formed by blockchain integrated with machine learning provides an enhanced system that resists multiple kinds of cyberattacks effectively. Improving performance capability of machine learning models as well as investigating novel blockchain security protocols must be pursued along with an assessment of deployment scalability for integrated solutions in massive IoT systems.

6. CONCLUSION

The combination of blockchain technology with machine learning functions as a robust method to boost IoT cybersecurity for distributed information technology systems that rely on IoT. This method combines these technologies to build an overall solution which confronts IoT-specific security issues effectively. A secure and resilient IoT environment emerges from blockchain-based access control which teams up with machine learning-based intrusion detection systems to support IoT application adoption and innovation. The combination of blockchain technology with IoT produces potential answers to enhance IoT security measures. Blockchain offers trustful inter-company partnerships to IoT because its decentralized public database enables user-based audit capabilities. Current research on blockchain applications for the IoT shows extensive progress but developing this technology to enhance security and privacy needs of IoT alongside cyber-security concerns remains in its early development phase. Blockchain technology utilizes its immutable nature together with its transparent features to verify data authenticity and track origins simultaneously with machine learning tools which recognize security irregularities and generate automated security protocols for protection. The research establishes a useful guide which directs organizations through their implementation of blockchain and machine learning-based security solutions for their Internet of Things projects. The research should proceed in three

directions: (1) exploring federated learning for machine learning model protection and privacy enhancement and (2) establishing blockchain-based security protocols for IoT devices along with (3) analyzing full-scale IoT analytics utilizing the integrated framework.

7. REFERENCES

[1] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," Ad Hoc Networks, vol. 11, no. 8, p. 2661, May 2013, doi: 10.1016/j.adhoc.2013.04.014.

[2] M. Shurman, R. M. Khrais, and A. Yateem, "DoS and DDoS Attack Detection Using Deep Learning and IDS," The International Arab Journal of Information Technology, vol. 17, p. 655, Jul. 2020, doi: 10.34028/iajit/17/4a/10.

[3] Kumar, D., Pawar, P., Gonaygunta, H., & Singh, S. (2023). Impact of federated learning on industrial iot-A Review. Int. J. Adv. Res. Comput. Commun. Eng, 13(1), 1-12.

[4] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning," arXiv (Cornell University), Jan. 2018, doi: 10.48550/arXiv.1801.06275.

[5] A. Mathur, T. Newe, W. Elgenaidi, M. Rao, G. Dooly, and D. Toal, "A secure end-to-end IoT solution," Sensors and Actuators A Physical, vol. 263, p. 291, Jun. 2017, doi: 10.1016/j.sna.2017.06.019.

[6] S. Bharati and P. Podder, "Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions," Security and Communication Networks, vol. 2022, p. 1, Aug. 2022, doi: 10.1155/2022/8951961.

[7] N. Waheed and M. Usman, "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures." Feb. 2023. Accessed: Apr. 23, 2025. [Online]. Available: https://www.semanticscholar.org/paper/Security-and-Privacy-in-IoT-Using-Machine-Learning-Waheed-Usman/346dc80571d13880a87bbf341577d6eb83414911

[8] Kumar, D., & Singh, S. (2024). Analyzing the impact of machine learning algorithms on risk management and fraud detection in financial institutions. International Journal of Research Publication and Reviews, 5(5), 1797-1804.

[9] E. P. Moro, "Distributed Ledger Technologies and the Internet of Things: A Devices Attestation System for Smart Cities," The Journal of British Blockchain Association, vol. 3, no. 1, p. 1, Apr. 2020, doi: 10.31585/jbba-3-1-(7)2020.

[10] N. T. Lam, "Detecting Unauthorized Network Intrusion based on Network Traffic using Behavior Analysis Techniques," International Journal of Advanced Computer Science and Applications, vol. 12, no. 4, Jan. 2021, doi: 10.14569/ijacsa.2021.0120407.

[11] P. Giudici, "Fintech Risk Management: A Research Challenge for Artificial Intelligence in Finance," Frontiers in Artificial Intelligence, vol. 1, Nov. 2018, doi: 10.3389/frai.2018.00001.

[12] Pillai, S. E. V. S., Polimetla, K., Prakash, C. S., Pareek, P. K., & Pawar, P. P. (2024, April). IoT Security Detection and Evaluation for Smart Cyber Infrastructures Using LSTMs with Attention Mechanism. In 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-5). IEEE.

[13] K. Arumugam et al., "Federated Transfer Learning for Authentication and Privacy Preservation Using Novel Supportive Twin Delayed DDPG (S-TD3) Algorithm for IIoT," Sensors, vol. 21, no. 23, p. 7793, Nov. 2021, doi: 10.3390/s21237793.

[14] Pawar, P. P., Kumar, D., Bhujang, R. K., Pareek, P. K., Manoj, H. M., & Deepika, K. S. (2024, July). Investigation on Digital Forensic Using Graph Based Neural Network with Blockchain Technology. In 2024 International Conference on Data Science and Network Security (ICDSNS) (pp. 1-7). IEEE.

[15] G. G. Samatas, S. S. Moumgiakmas, and G. A. Papakostas, "Predictive Maintenance -- Bridging Artificial Intelligence and IoT," arXiv (Cornell University), Jan. 2021, doi: 10.48550/arXiv.2103.11148.

[16] Kumar, D. (2022). Factors Relating to the Adoption of IoT for Smart Home. University of the Cumberlands.

[17] A. Wood, K. Najarian, and D. Kahrobaei, "Homomorphic Encryption for Machine Learning in Medicine and Bioinformatics," ACM Computing Surveys, vol. 53, no. 4. Association for Computing Machinery, p. 1, Jul. 07, 2020. doi: 10.1145/3394658.

[18] N. Ansar, M. S. Ansari, M. Sharique, A. Khatoon, M. A. Malik, and M. M. Siddiqui, "A Cutting-Edge Deep Learning Method For Enhancing IoT Security," arXiv (Cornell University), Jun. 2024, doi: 10.48550/arxiv.2406.12400.

[19] M. A. Bouras, B. Xia, A. O. Abuassba, H. Ning, and Q. Lu, "IoT-CCAC: a blockchain-based consortium capability access control approach for IoT," PeerJ Computer Science, vol. 7, Apr. 2021, doi: 10.7717/peerj-cs.455.

[20] N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by Blockchain: Safeguarding Internet of Things Devices," IEEE Consumer Electronics Magazine, vol. 8, no. 3, p. 28, Apr. 2019, doi: 10.1109/mce.2019.2892221.

[21] X. Wang and X. Lu, "A Host-Based Anomaly Detection Framework Using XGBoost and LSTM for IoT Devices," Wireless Communications and Mobile Computing, vol. 2020, p. 1, Oct. 2020, doi: 10.1155/2020/8838571.

[22] A. A. Shorman, H. Faris, and I. Aljarah, "Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection," Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 7, p. 2809, Jul. 2019, doi: 10.1007/s12652-019-01387-y.

[23] Pawar, P. P., Kumar, D., Ananthan, B., Pradeepa, A. S., & Selvi, A. S. (2024, May). An efficient ddos attack detection using attention based hybrid model in blockchain based SDN-IOT. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-5). IEEE.

[24] Maturi, M. H. (2024). Optimizing energy efficiency in edge-computing environments with dynamic resource allocation. environments, 13(07), 01-08.

[25] Mohamed, H., Koroniotis, N., Schiliro, F., & Moustafa, N. (2025). IoT-CAD: A comprehensive Digital Forensics dataset for AI-based Cyberattack Attribution Detection methods in IoT environments. Ad Hoc Networks, 103840.

[26] Pawar, P. (2022). Factors Influencing Blockchain Technology Adoption in Supply Chain (Doctoral dissertation, University of the Cumberlands).